EXHIBIT 2

| | |
|---|---|
| STATE OF MINNESOTA | IN DISTRICT COURT |
| COUNTY OF HENNEPIN | FOURTH JUDICIAL DISTRICT<br>Case Type: Civil |

GUAVA LLC,

Plaintiff,

vs.

SPENCER MERKEL,

Defendant.

Court File No.
Judge:

**COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff Guava LLC, by and through its undersigned counsel, hereby files this Complaint requesting damages and injunctive relief, and alleges as follows:

## INTRODUCTION

1. Plaintiff files this action for interception of electronic communications and civil conspiracy, arising from unlawful computer breaches. By this action, Guava seeks compensatory damages, injunctive relief and attorney's fees and costs.

## PARTIES

2. Plaintiff is a limited liability company that owns and operates protected computer systems, including computer systems accessible throughout Minnesota.

3. Defendant Spencer Merkel breached Plaintiff's protected computer systems and intercepted Plaintiff's electronic communications.

## BACKGROUND

4. Hacking has become a serious threat to anyone maintaining private or protected computer systems. *See* Kevin Parrish, *Hackers Have Access to 1 in 5 Microsoft Logins*, TOM'S GUIDE, July 16, 2012, attached hereto as Exhibit A (finding that "20-percent of

Microsoft Account logins are found on lists of compromised credentials stemming from hack attacks on other services like Yahoo and Facebook."); Michael Mimoso, *Cybercrime Gang Recruiting Botmasters for Large-Scale MiTM Attacks on American Banks*, THE THREAT POST, Oct. 4, 2012, attached hereto as Exhibit B (explaining that "[a]s many as 30 banks have been targeted" recently by cyber hackers.); Bryon Acohido, *No Slowdown in Sight for Cyberattacks*, USA TODAY, July 30, 2012, attached hereto as Exhibit C (Eddie Schwartz, chief security officer of security firm RSA stating that "[i]t's easier and safer for a criminal to steal money from an online bank account, rather than have to walk into a bank — or to steal intellectual property in an online setting, rather than have to send in a human spy.").

5. Even large corporations and governmental agencies are not immune from hacking attacks. *See* Kim Zetter, *Hackers Release 1 Million Apple Device IDs Allegedly Stolen From FBI Laptop*, WIRED, Sept. 4, 2012, attached hereto as Exhibit D (explaining that a hacker group obtained "1 million Apple device IDs that" were "obtained from an FBI computer they hacked.").

6. Companies harmed by hacking are encouraged to seek relief in the courts. *See* Glenn Chapman, *Cyber Defenders Urges to go on the Offense*, AMERICAN FREE PRESS, July 26, 2012, attached hereto as Exhibit E (former FBI cyber crime unit chief Shawn Henry explaining that "I believe the threat from computer network attack is the most significant threat we face as a civilized world, other than a weapon of mass destruction." and Black Hat founder Jeff Moss proposing that "cyber attackers also be fought on legal fronts, with companies taking suspected culprits to court.").

## FACTUAL ALLEGATIONS

7. Plaintiff operates computer systems that distribute third-party content. By way of analogy, Plaintiff is like a satellite radio station in that it distributes content owned by others. Plaintiff generates revenue by requiring third-parties to pay a fee for accessing its distributions systems. Members are assigned a username and password in order to access the distribution system.

8. Defendant used a username and password that did not belong to him to gain unauthorized access to Plaintiff's protected computer systems. Once he gained unauthorized access to Plaintiff's protected computer systems he intercepted electronic communications between Plaintiff and its legitimate members.

9. Defendant obtained the username and password he used to gain unauthorized access to Plaintiff's protected computer systems from a website that allows its members to trade stolen usernames and passwords amongst one another.

## COUNT I – INTERCEPTION OF ELECTRONIC COMMUNICATIONS

10. Plaintiff hereby incorporates by reference each and every allegation contained in the preceding paragraphs as if set forth fully herein.

11. Defendant used hacked usernames and passwords to gain access to Plaintiff's protected computer systems and intentionally intercepted numerous electronic communications between Plaintiff and its paying members.

12. The intercepted electronic communications included information regarding the identities of Plaintiff's customers, account information, financial information, computer programming and security information, and other information that Plaintiff protects and

does not even give access to third parties, even those who pay for and obtain legitimate passwords to access Plaintiff's websites.

13. Plaintiff has suffered actual damages as a result of Defendant's actions.

14. Defendant profited by the unauthorized interceptions of Plaintiff's electronic communications.

15. Those actions on the part of Defendant constitute violations of Minn. Stat. § 626A.02 Interception and Disclosure of Wire, Electronic, or Oral Communications Prohibited. A private right of action exists under Minn. Stat. § 626A.32.

## COUNT II – CIVIL CONSPIRACY

16. Plaintiff hereby incorporates by reference each and every allegation contained in the preceding paragraphs as if set forth fully herein.

17. Defendant colluded with multiple members of a hacking community to intercept electronic communications taking place on Plaintiff's protected computer systems. The hacking community's members share hacked usernames and passwords among other members to ensure that they had access to Plaintiff's protected computer systems.

18. Defendant reached an agreement with his fellow co-conspirators to gain unlawful access to Plaintiff's computer systems and intercept electronic communications. Defendant was aware that the hacked username and password he used did not belong to him and that he did not have Plaintiff's permission to access its computer systems and electronic communications.

19. Defendant committed overt tortious and unlawful acts by using hacked usernames and passwords to impermissibly obtain access to Plaintiff's protected computer systems and electronic communications.

20. As a proximate result of this conspiracy, Plaintiff has been damaged, as is more fully alleged above.

## JURY DEMAND

21. Plaintiff hereby demands a jury trial in this case.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays judgment and relief against Defendant as follows:

1) Judgment against Defendant that he or she has committed prohibited interception of Plaintiff's electronic communications pursuant to Minn. Stat. § 626A.02;

2) Judgment in favor of the Plaintiff against the Defendant for actual damages or statutory damages pursuant to Minn. Stat. § 626A.02 and common law, at the election of Plaintiff, in an amount in excess of $100,000 to be ascertained at trial;

3) On Count II, an order that Defendant is jointly and severally liable to the Plaintiff in the full amount of Judgment on the basis of a common law claim of civil conspiracy;

4) Judgment in favor of Plaintiff against the Defendant awarding the Plaintiff attorneys' fees, litigation expenses (including fees and costs of expert witnesses), and other costs of this action; and

5) Judgment in favor of the Plaintiff against Defendant, awarding Plaintiff declaratory and injunctive or other equitable relief as may be just and warranted.

Respectfully submitted,

Guava LLC

DATED: October 5, 2012

By:

Michael K. Dugas
Bar No. 0392158
Alpha Law Firm LLC
900 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (415) 325 – 5900
mkdugas@wefightpiracy.com
*Attorney for Plaintiff*

EXHIBIT A

# Hackers Have Access To 1 in 5 Microsoft Logins

9:00 PM - July 16, 2012 - By Kevin Parrish - Source : Microsoft

Twitter27 StumbleUpon0 Share63

**Microsoft blames the re-use of passwords for the high account hacking rate.**

ZoomEric Doerr, Group Program Manager for Microsoft's Account system, said on Sunday that 20-percent of Microsoft Account logins are found on lists of compromised credentials stemming from hack attacks on other services like Yahoo and Facebook. Naturally he slammed the use of providing the same passwords and login details across multiple services, saying that one breached service could mean multiple account hacks.

"These attacks shine a spotlight on the core issue – people reuse passwords between different websites," he said on Sunday. "This highlights the longstanding security advice to use unique passwords, as criminals have become increasingly sophisticated about taking a list of usernames and passwords from one service and then 'replaying' that list against other major account systems. When they find matching passwords they are able to spread their abuse beyond the original account system they attacked."

Doerr said that Microsoft regularly gets notified of lists of compromised external account info (email addresses and/or passwords from other networks) from different sources. These sources can include one of the many worldwide law enforcement agencies, an ISP, and even another company that runs an identity system. They contact Microsoft so that users are informed about a possible account hacking.

"You'd be surprised how often the lists – especially the publicly posted ones – are complete garbage with zero matches," Doerr said. "But sometimes there are hits – on average, we see successful password matches of around 20-percent of matching usernames. A recent one only had 4.5-percent overlap. This is actually exciting because it means that, on average, 80% of our customers are following safe password practices, and this reflects a growing sophistication in our customers."

He said when Microsoft receives a list, the company checks to see if it actually matches any accounts and passwords in the system through an automated hands-off process. Then the company looks to see if there is any evidence of criminal activity like sending spam. If there are signs of criminal activity, then the account is suspended until the owner goes through the recovery process.

"Occasionally we get information about a set of customers, but there isn't enough account information to identify who has reused passwords and is therefore at risk," he said. "Then we have a judgment call – do we ask 100-percent of those customers to reset their passwords, even though only 20-percent are probably at risk? Or do we leave the 20-percent at risk to avoid inconveniencing the 80-percent?"

Where there is a credible threat, Microsoft would rather inconvenience 100-percent of the customers by resetting all passwords, he said.

Currently the team is working on beefing up security by offering increased password lengths. "Unfortunately, for historical reasons, the password validation logic is decentralized across different products, so it's a bigger change than it should be and takes longer to get to market," he added. "It's also worth noting that the vast majority of compromised accounts are through malware and phishing. The small fraction of brute force is primarily common passwords like '123456' not due to a lack of complexity."

# EXHIBIT B

October 4, 2012, 12:15PM

# Cybercrime Gang Recruiting Botmasters for Large-Scale MiTM Attacks on American Banks

by Michael Mimoso

A slew of major American banks, some already stressed by a stream of DDoS attacks carried out over the past 10 days, may soon have to brace themselves for a large-scale coordinated attack bent on pulling off fraudulent wire transfers.

RSA's FraudAction research team has been monitoring underground chatter and has put together various clues to deduce that a cybercrime gang is actively recruiting up to 100 botmasters to participate in a complicated man-in-the-middle hijacking scam using a variant of the proprietary Gozi Trojan.

This is the first time a private cybercrime organization has recruited outsiders to participate in a financially motivated attack, said Mor Ahuvia, cybercrime communications specialist for RSA FraudAction. The attackers are promising their recruits a cut of the profits, and are requiring an initial investment in hardware and training in how to deploy the Gozi Prinimalka Trojan, Ahuvia added. Also, the gang will only share executable files with their partners, and will not give up the Trojan's compilers, keeping the recruits dependent on the gang for updates

Generally, cybercrime gangs deploy as few as five individual botmasters to help in successful campaigns; with this kind of scale, banks could be facing up 30 times the number of compromised machines and fraudulent transfers, if the campaign is successful.

"This Trojan is not well known. This is not SpyEye or Citadel; it's not available for everyone to buy," Ahuvia said. "Security vendors and antivirus signatures are less likely to catch it or be familiar with it. It will be tricky for vendors to detect and block it. This gang is keeping a tight hold on the compiler. By only giving up executable files, they can control how any antivirus signatures are in the wild and keep unique signatures to a minimum."

As many as 30 banks have been targeted, many of them well known and high profile, Ahuvia said. RSA said the gang is targeting American banks because of past success in beating their defenses, as well as a lack of two-factor authentication required for wire transfers.Some European banks, for example, require consumers to use two-factor authentication. She added that RSA FraudAction was unsure how far along the recruitment campaign had gone, or when the attacks would launch.

"There is the chance that once we've gone public, they may abandon their plans because there's too much buzz around it," Ahuvia said. "On the other hand, I don't think anything we know will have such a dramatic effect on them. There are so many Trojans available and so many points of failure in security that could go wrong, that they'd still have some chance of success."

RSA's researchers were able to make the connection to the Gozi Prinimalka Trojan, which has been in circulation since 2008 and responsible for $5 million in fraud-related losses. Prinimalka is similar to the Gozi Trojan in technical and operational aspects, RSA said, leading to speculation the HangUp Team, which was tied to previous Gozi attacks, is behind this attack as well. Prinimalka is Russian for the word "receive" and is a folder name in every URL patch given by this particular gang to its crimeware servers.

Prinimalka uses the same bot-to-server communication pattern and URL trigger list as Gozi, RSA said. But deployment of the two Trojans is different: Gozi writes a single DLL file to bots upon deployment, while Prinimalka writes two, an executable file and a DAT file which reports to the command and control server.

Once the Trojan is launched, the botmaster fires up a virtual machine synching module. The module then duplicates the victim's computer, including identifiable features such as time zone, screen resolution, cookies, browser type and version, and software identification, RSA said. This allows the botmaster to impersonate the victim's machine and access their accounts. Access is carried out over a SOCKS proxy connection installed on the victim's machine, RSA said.

The cloned virtual system then can move about on the genuine IP address of the compromised machine when accessing the bank website. Taking it a step further, the attackers deploy VoIP phone flooding software that will prevent the victim from receiving a confirmation call or text alerting them to unusual transfer activity, RSA said.

"They are looking for this to be a quick campaign," Ahuvia said. "They want to make as much as they can until the banks and users harden their systems. They want to cash out quickly."

*Commenting on this Article will be automatically closed on January 4, 2013.*

# EXHIBIT C

# No slowdown in sight for cyberattacks

By Byron Acohido, USA TODAY

Updated 7/30/2012 10:03 AM

Recommend 0 102 2

Reprints & Permissions

LAS VEGAS - Cyber attacks are accelerating at a pace that suggests the Internet - already a risky environment - is likely to pose a steadily growing threat to individuals and companies for years to come.

Getty Images

Internet-generated attacks comprise the most significant threat we face as a civilized world, other than a weapon of mass destruction,' according to one security expert

That's the somber consensus of security and Internet experts participating in the giant Black Hat cybersecurity conference that concluded here this week.

Internet-generated attacks comprise "the most significant threat we face as a civilized world, other than a weapon of mass destruction," Shawn Henry, former head of the FBI's cybercrime unit, told some 6,500 attendees in a keynote address.

Joe Stewart, Dell SecureWorks' director of malware research, presented research detailing the activities of two large cyber gangs, one based in Shanghai the other in Beijing, that have cracked into the networks of thousands of companies over the past half dozen years.

The attacks invariably begin by infecting the computer of one employee, then using that machine as a toehold to patiently probe deep into the company's network. The end game: to steal customer lists, patents, bidding proposals and other sensitive documents.

Videos you may be interested in

second chance at MLB at-bat

debates make a difference?

Strange Bean Burns Fat"
[illegible]

by Taboola
More videos

Most Popular

Stories
- HF Test
- Don't fall for Facebook 'privacy' notice
- Smart Office 2: A versatile software suite

Videos
- Ed Baig reviews Kindle Paperwhite
- 'Pregnant man' struggles through nasty divorce
- Tennis Channel Court Report 9-30-2012

Photos
- Mayan calendar discovery
- Facebook
- Apple iPhone 5 first day sales

Each gang is made up of dozens of employees playing complementary roles in attacks that are "stealthy and persistent," says Stewart. "Even if they do get discovered and get kicked out of a network, they come back, targeting a different employee."

Another gang, analyzed by Dell SecureWorks' researcher Brett Stone-Gross, has been blasting out spam, designed to slip past spam filters. The messages carry instructions to click on a link to read bogus delivery invoices, airline reservations or cellphone bills. The link, however, takes the user to a web page that installs malicious software.

Stone-Gross said the gang currently has access to 678,000 infected PCs, some of which are used to carry out its lucrative specialty: orchestrating fraudulent wire transfers from online banking accounts.

Meanwhile, a different category of hackers is stepping up attacks, not on individual PCs, but on company websites. Website attacks now routinely occur thousands of times each, as criminals probe for ways to breach databases carrying usernames and passwords and other valuable data, says David Koretz, general manager of website security firm Mykonos, a division of Juniper Networks.

Some successful website hackers enjoy boasting —-by publically posting some, if not most, of the stolen data. That's happened recently with data stolen from online retailer Zappos, matchmaking site eHarmony, business social networking site LinkedIn and search giant Yahoo, Koretz says.

Experts say web attacks continue to escalate partly because powerful, easy-to-use hacking programs are widely available for free. What's more, opportunities for an intruder to take control of an individual's PC, or access and probe a company's network, are multiplying as society uses more Internet-delivered services and Internet-connected mobile devices.

"It's easier and safer for a criminal to steal money from an online bank account, rather than have to walk into a bank — or to steal intellectual property in an online setting, rather than have to send in a human spy," says Eddie Schwartz, chief security officer of security firm RSA, a division of EMC.

*For more information about reprints & permissions, visit our FAQ's. To report corrections and clarifications, contact Standards Editor* **Brent Jones**. *For publication consideration in the newspaper, send comments to letters@usatoday.com. Include name, phone number, city and state for verification. To view our corrections, go to corrections.usatoday.com.*

Posted 7/27/2012 10:34 AM | Updated 7/30/2012 10:00 AM

Most Popular E-mail Newsletter

Sign up to get:

Top viewed stories, photo galleries and community posts of the day

Most popular right now:
HF Test

USA TODAY MOST POPULAR

Sign up for USA TODAY E-mail newsletters

More from USATODAY

Man kills girlfriend for revealing she was HIV positive *USATODAY.COM in On Deadline*

More Duchess Kate topless pics out; police hunt photographer *USATODAY.COM in LifeLine Live*

Column: Christian companies can't bow to sinful mandate *USATODAY.COM in News*

5 reasons to skip iPhone 5 lines *USATODAY.COM in Tech*

*USA TODAY is now using Facebook Comments on our stories and blog posts to provide an enhanced user experience. To post a comment, log into Facebook and then "Add" your comment. To report spam or abuse, click the "X" in the upper right corner of the comment box. To find out more, read the FAQ and Conversation Guidelines.*

# EXHIBIT D

Threat Level
Privacy, Crime and Security Online
Hacks and Cracks
Cybersecurity

Like 213 85 22 Share 14

# Hackers Release 1 Million Apple Device IDs Allegedly Stolen From FBI Laptop

By Kim ZetterEmail Author
09.04.12
12:49 PM
Follow @KimZetter

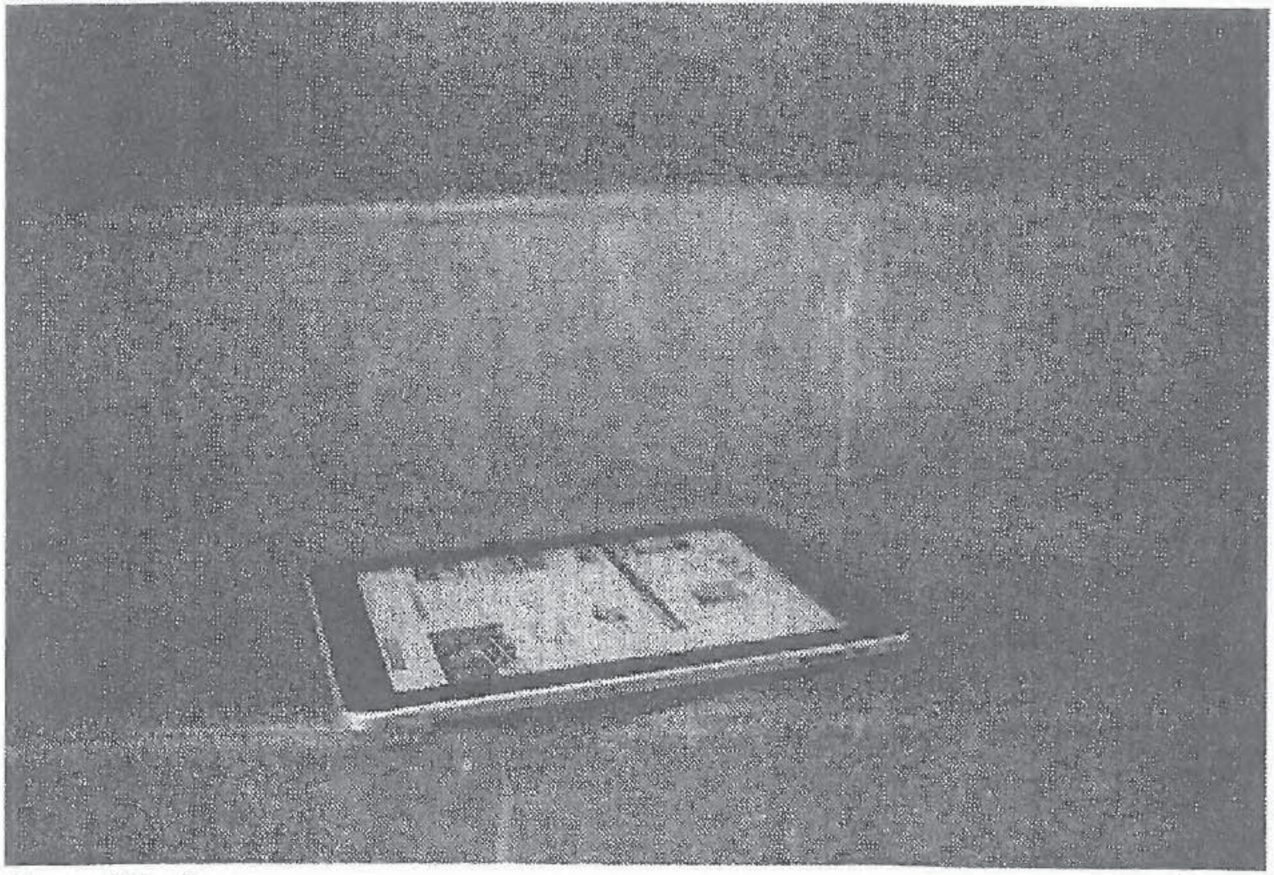


*Photo: Wired*

The hacker group AntiSec has released 1 million Apple device IDs that they say they obtained from an FBI computer they hacked.

The hackers say they actually stole 12 million IDs, including personal information, from the hacked FBI computer, but released only 1 million in an encrypted file published on torrent sites.

In a lengthy post online, the hackers wrote that last March, they hacked a laptop belonging to an FBI agent named Christopher K. Stangl from the bureau's Regional Cyber Action Team and the New York FBI office's Evidence Response Team.

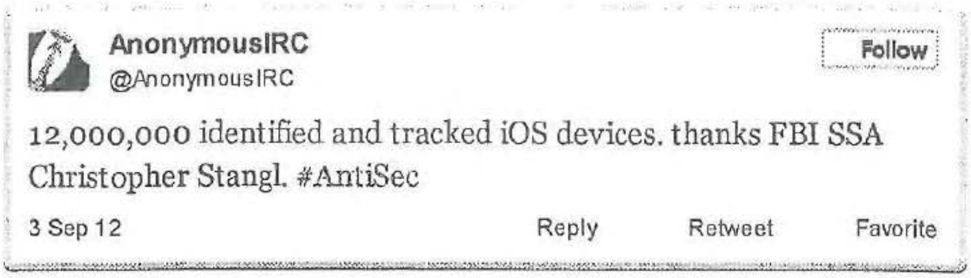
The hackers say the IDs were stored in a file on Stangl's desktop titled "NCFTA_iOS_devices_intel.csv."

Filed in Fourth Judicial District Court
10/17/2012 3:07:20 PM
Hennepin County Civil, MN

The file, according to the hackers, contained a list of more than 12 million Apple iOS devices, including Unique Device Identifiers (UDID), user names, names of devices, types of devices, Apple Push Notification Service tokens, ZIP codes, cellphone numbers, and addresses. The hackers released only 1 million UDIDs, however, and did not release the accompanying personal information for the IDs.

Apple UDIDs are a 40-character alphanumeric string that is unique to each Apple device.

It's not known why the FBI possessed the Apple IDs. The hackers suggested in a tweet from the the @AnonymousIRC account, that the FBI was using the information to track users.



12,000,000 identified and tracked iOS devices. thanks FBI SSA Christopher Stangl. #AntiSec

3 Sep 12

Stangl may have been targeted because he was on an e-mail that members of Anonymous intercepted last January. The e-mail was sent to several dozen U.S. and European law-enforcement personnel to participate in a conference call discussing efforts to investigate Anonymous and other hacking groups. The email included a call-in number for the discussion, which members of Anonymous recorded and posted online last February.

The hackers say they released the Apple UDIDs so that people would know that the FBI may be tracking their devices and also because, they wrote in their online post, "we think it's the right moment to release this knowing that Apple is looking for alternatives for those UDID currently ... but well, in this case it's too late for those concerned owners on the list."

Apple has been criticized for hard-coding the ID's in devices, since they can be misused by application developers and others to identify a user, when combined with other information, and track them. Last April, Apple began rejecting applications that track UDIDs.

The Next Web has created a tool for users to check if their Apple UDID is among those that the hackers released.

Related

You Might Like

Related Links by Contextly

# EXHIBIT E

# Cyber defenders urged to go on the offense

By Glenn Chapman (AFP) – Jul 26, 2012

LAS VEGAS — Computer security champions on Wednesday were urged to hunt down and eliminate hackers, spies, terrorists and other online evildoers to prevent devastating Internet Age attacks.

The first day of briefings at a prestigious Black Hat computer security gathering here opened with a former FBI cyber crime unit chief calling for a shift from defense to offense when it comes to protecting networks.

"We need warriors to fight our enemies, particularly in the cyber world right now," Shawn Henry said in a Black Hat keynote presentation that kicked off with dramatic video of hostage rescue teams training.

"I believe the threat from computer network attack is the most significant threat we face as a civilized world, other than a weapon of mass destruction."

The peril grows as water supplies, power grids, financial transactions, and more rely on the Internet and as modern lives increasingly involve working and playing on smartphones or tablet computers, according to Henry.

He rolled off a list of adversaries ranging from spies and well-funded criminals to disgruntled employees with inside knowledge of company networks.

"Cyber is the great equalizer," Henry said.

"With a $500 laptop with an Internet connection anybody, anywhere in the world can attack any organization, any company," he continued. "The last time I checked, that was about 2.3 billion people."

After 24 years of working for the FBI, Henry in April switched to the private sector as the head of a division at startup CrowdStrike specializing in cyber attack incident responses and identifying adversaries.

The computer security industry to expand its arsenal beyond just building walls, filters and other safeguards against online intruders to include watching for, and gathering intelligence on, culprits who have slipped through.

"It is not enough to watch the perimeter," Henry said, equating computer security to protecting real world offices. "We have to be constantly hunting; looking for tripwires."

In the cyber world, that translates into monitoring system activities such as whether files have been accessed or changed and by whom.

"The sophisticated adversary will get over that firewall and walk around, like an invisible man," Henry said. "We have to mitigate that threat."

Tactics for fighting cyber intruders should include gathering information about how they operate and the tools used, and then sharing the data in the industry and with law enforcement agencies in relevant countries.

"Intelligence is the key to all of this," Henry said. "If we understand who the adversary is, we can take specific actions."

Teamwork between governments and private companies means that options for responding to identified cyber attackers can range from improved network software to political sanctions or even military strikes, according to Henry.

"You can't make every school, every mall, every university, and every workplace impenetrable," Henry said. "We have to look at who the adversary is and stop them in advance of them walking in."

Black Hat founder Jeff Moss, the self-described hacker behind the notorious Def Con gathering that starts here on Thursday, backed Henry's argument.

"Maybe we need some white blood cells out there; companies willing to push the edge and focus on threat actors," Moss said, calling on the computer security community to "raise the immunity level."

Moss is head of security at the Internet Corporation for Assigned Names and Numbers, which oversees the world's website addresses.

"So, am I Luke, or am I Darth Vader; sometimes I'm not sure," Moss quipped about his roles in the hacker realm and the computer security industry.

"It depends upon which day and who asks."

Moss proposed that cyber attackers also be fought on legal fronts, with companies taking suspected culprits to court.

"I can't print money; I can't raise an army, but I can hire lawyers and they are almost as good," Moss said. "One way to fight the enemy is you just sue them."

Henry feared that it may take an Internet version of the infamous 9/11 attack in New York City to get the world to take the cyber threat to heart.

"We need to get down range and take them out of the fight," Henry said.

Former FBI cyber crime unit chief Shawn Henry was the keynote speaker at the Black Hat computer security gathering (AFP/Getty Images/File)

## Map

"As well-trained, well-equipped cyber warriors you can have an impact; the stakes are high."

More »

Add News to your Google Homepage

©2012 Google - About Google News - Blog - Help Center - Help for Publishers - Terms of Use - Privacy Policy - Google Home